ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

July 4, 2026

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 6:00 AM (EDT) on July 2, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Weekly Intelligence Brief

This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – DeadLock's Ransomware Leak Site Lists over 80 Victims

On June 16, 2026, ZeroFox observed a ransomware leak site titled "DeadLock" that listed roughly 80 victims. About 57 percent of the total observed claimed victims are located in the Europe-Russia region, while Asia-Pacific (APAC), North America, South America, and the Middle East and Africa collectively account for the remainder of the listings. ZeroFox assesses that the group is very likely primarily focused on extracting ransom amounts from the listed entities rather than establishing its presence in the cybercrime ecosystem. ZeroFox assesses that the group's widespread regional and industry targeting, availability of data download links, and reported campaign techniques indicate a roughly even chance that many listed victims were legitimately impacted.

ZeroFox Intelligence Profile – ICARUS

ZeroFox first observed ransomware and digital extortion (R&DE) collective ICARUS's data leak site (DLS) and associated extortion campaigns in late April to early May 2026. Since becoming active, the group has listed at least three confirmed targets and five additional redacted entities on its DLS, suggesting ongoing and expanding operations as of mid-2026. The operators of "The Underground _ Uwu" Telegram channel have reposted ICARUS's original leak post and have previously claimed affiliations with Scattered Lapsus$ Hunters (SLH); this raises the possibility of an affiliation between ICARUS and SLH. However, ICARUS has not publicly acknowledged or claimed any such affiliation. ICARUS is very likely financially motivated. Neither its DLS communications nor its observed operational behavior indicate any political stance, ideological messaging, or affiliation with a specific cause. ZeroFox has observed that ICARUS employs a multitiered extortion model centered on supply chain compromise, data exfiltration, and public disclosure threats. ZeroFox assesses that ICARUS is likely an operationally immature threat actor group based on multiple observed operational security (OPSEC) lapses. Despite presenting a polished public-facing DLS, the group's operational conduct reflects significant inconsistencies that suggest limited experience relative to more established R&DE collectives.

ZeroFox Intelligence Flash Report – Online Impersonations Likely to Spike in July

ZeroFox assesses that impersonation volume is likely to spike in July 2026, consistent with our observed seasonal patterns in the previous reporting period. Between May 1, 2025, and April 30, 2026,

ZeroFox executed 1,412,243 client-requested takedowns across all monitored network categories, which represents a significant volume of disruption activity on behalf of its customer base. ZeroFox observed a significant peak in impersonation volume in Q3 2025, with July 2025 recording the highest single-month total of 191,078 takedowns. This figure was driven predominantly by social media activity, which accounted for the largest share of our takedown submissions throughout the year. Following the summer 2025 peak, ZeroFox noted a gradual decline in our overall takedown volume through the fall before a secondary elevation in December 2025. Notably, this was driven by an anomalous spike in peer-to-peer (P2P) and communications activity—a category that otherwise tracked at moderate and relatively stable volumes.

ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 14

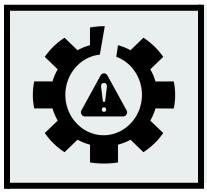
The Underground Economist is an intelligence-focused series illuminating Dark Web findings in digestible tidbits from our ZeroFox Dark Ops intelligence team.

Monthly Geopolitical Report July 2026

War in Iran has likely altered the shipping landscape permanently. Repeated closures of the Strait of Hormuz (SoH) will almost certainly continue to erode customer confidence pertaining to goods shipped throughout the region. Iran's nuclear and missile programs and its support for regional proxy groups such as Hezbollah will all but certainly be additional sticking points as talks aimed at peace in the region progress. An extension of the initial 60-day negotiation period agreed to in the Memorandum of Understanding (MOU) between the United States and Iran is all but certain. The Group of Seven (G7) concluded its annual summit with a public commitment to diversify trade networks away from China, which will very likely be followed by European Union (EU) efforts to address its growing trade imbalance with China. Recent data on trade between China and the United States and Japan very likely signals the forms Chinese retaliation will take.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



Boeing IT Outage Disrupts Commercial and Military Operations

What we know:

- On June 30, 2026, aerospace company Boeing reportedly experienced an IT outage that affected its commercial and military operations.
- Boeing said it had no reason to believe the outage was caused by a cyberattack.

Background:

- The outage reportedly disrupted some of Boeing's computer systems and applications, affecting commercial jet inspections and paperwork.
- At the time of writing, Boeing has not confirmed that the outage has been fully resolved, although normal operations are resuming at multiple affected facilities.

Analyst note:

- Threat actors are likely to exploit the incident by launching social engineering campaigns impersonating Boeing IT support and urging employees to execute commands and deploy malicious files in the guise of restoring affected systems.

Apple's iPhone 18 Pro Supply Chain Data Leaked in Tata Electronics Incident

What we know:

- Files detailing Apple's supplier list and component specifications for the unreleased iPhone 18 Pro and Pro Max were reportedly part of those posted to the dark web in the Tata Electronics breach claimed by World Leaks ransomware group.

Background:

- The exposed data discloses supplier mappings that Apple does not make public, along with details on chips, battery components, and camera parts.
- The files reportedly carry "confidential" watermarks and internal code names associated with the iPhone 18 Pro series.

Analyst note:

- The exposure of unreleased supplier and product data will very likely provide competitors with insight into Apple's guarded sourcing strategies and deepen supply chain risk ahead of the iPhone 18 Pro's anticipated September 2026 launch.
- This incident is also likely to further strain the Apple-Tata relationship at a critical point in Apple's expansion of manufacturing in India.

Authorities Seize Nearly 400 Domains Illegally Streaming FIFA World Cup Matches

What we know:

- The United States and its partners have seized nearly 400 domains illegally streaming Fédération Internationale de Football Association (FIFA) World Cup Finals matches in violation of U.S. copyright law, as part of Operation Offsides.

Background:

- Servers and domains were targeted in Peru and Bulgaria, while additional disruptions took place in Croatia, Romania, Poland, and Colombia.
- Apart from violating intellectual property rights, illegal streaming sites also fuel criminal organizations and expose viewers to threats such as malware infections and unsecure connections that can compromise personal and financial data.

Analyst note:

- The multinational law enforcement operation suggests that illegal streaming platforms are very likely operated by transnational organized crime groups.
- Profits from these operations are likely to finance broader criminal activities.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added two vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on June 29 and July 1, 2026. Additionally, on June 30, 2026, CISA released eight Industrial Control Systems (ICS) advisories, including CVE-2026-12819, CVE-2026-50110, CVE-2026-9650, and CVE-2026-50003. Apple has released patches for over 30 vulnerabilities across Kernel, WebKit, WebRTC, and libxslt components. CVE-2026-20245 is a now-patched privilege escalation vulnerability in Cisco Catalyst SD-WAN that was exploited as a zero-day. Adobe has released security updates for multiple vulnerabilities affecting Adobe ColdFusion and Adobe Campaign Classic. Attackers are actively exploiting a critical authentication bypass flaw in SimpleHelp that can enable them to obtain authenticated access by forging certain tokens.

CRITICAL

CVE-2026-46817

What happened: A critical vulnerability in the File Transmission component of Oracle E-Business Suite (EBS)'s Oracle Payments product is being actively exploited.

- **What this means:** The flaw enables an unauthenticated attacker with HTTP network access to take over vulnerable systems through low-complexity attacks. Oracle released a fix for the vulnerability as part of its May 2026 Critical Security Patch Update.

  Affected products: Oracle E-Business Suite versions 12.2.3-12.2.15

HIGH

CVE-2026-12957

What happened: This is a high-severity flaw in Amazon's artificial intelligence (AI) coding assistant for Visual Studio Code (VS Code) that enables arbitrary code execution and credential theft.

- **What this means:** Attackers are likely to gain unauthorized access to Amazon Web Services (AWS) credentials, Application Programming Interface (API) keys, authentication tokens, and Secure Shell (SSH) agent sockets.

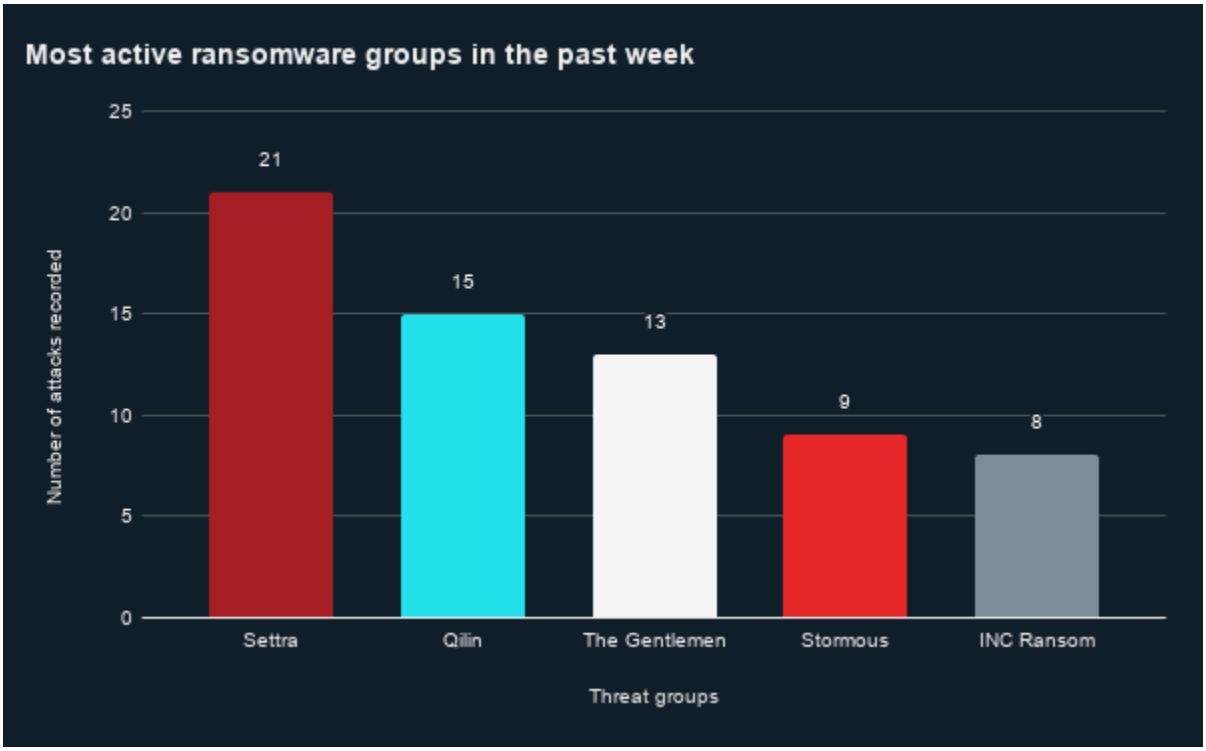
Affected products: The affected products are listed here.

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

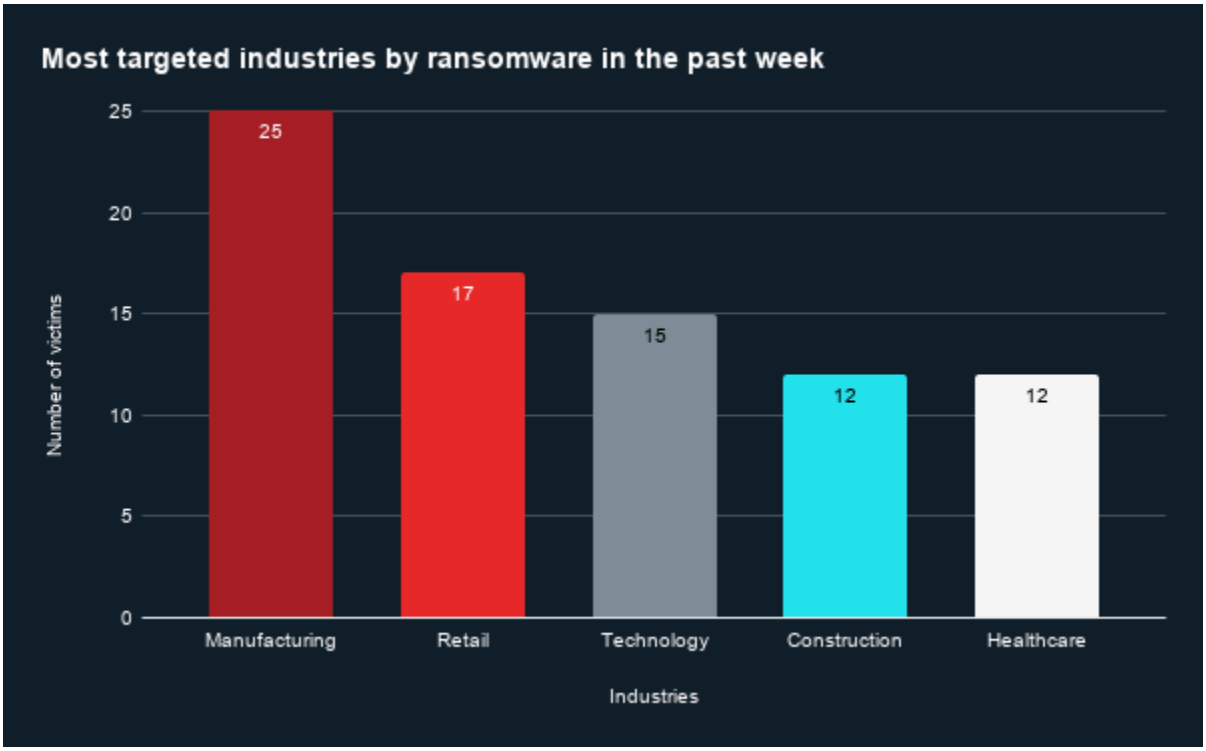
Ransomware Group, Industry, and Regional Trends

Last week in ransomware: In the past week, Settra, Qilin, The Gentlemen, Stormous, and INC Ransom were the most active ransomware groups. ZeroFox observed close to 122 ransomware victims disclosed, most of whom were located in North America. The Settra ransomware group accounted for the largest number of attacks, followed by Qilin.



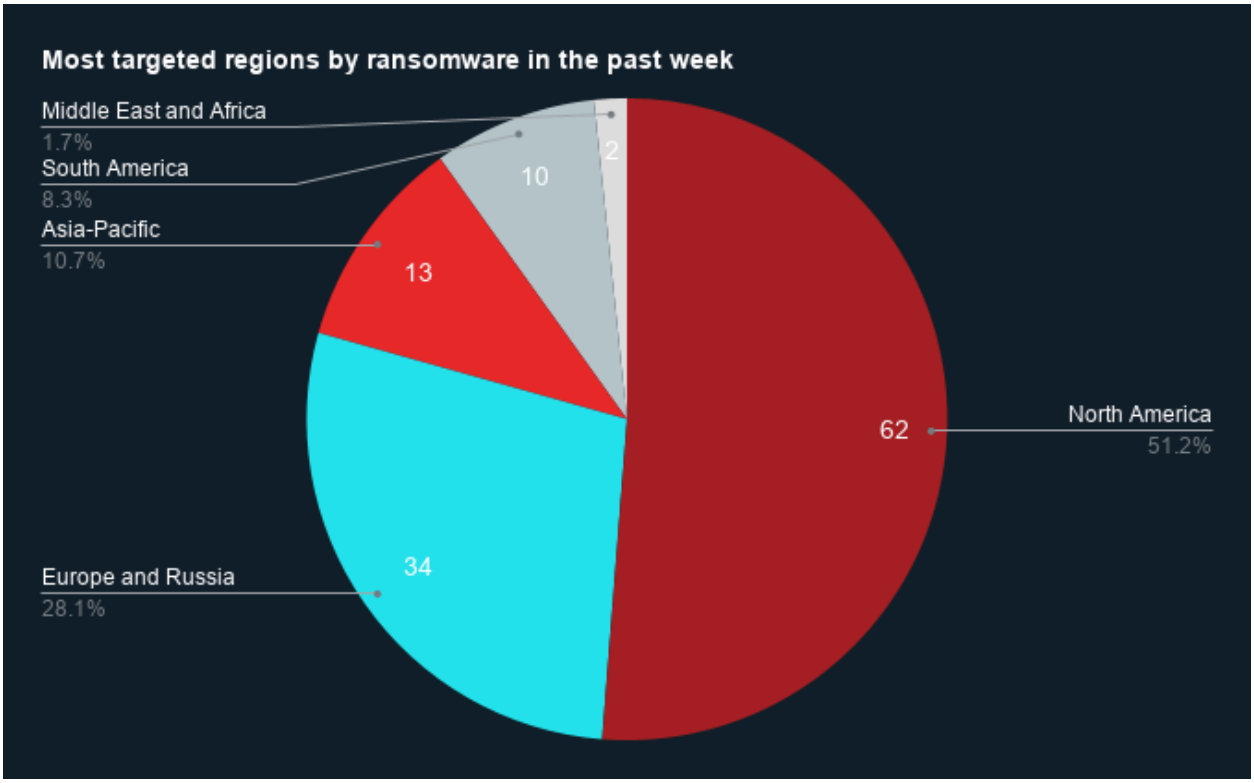
Source: ZeroFox Internal Collections

Industry ransomware trends: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by retail.



Source: ZeroFox Internal Collections

Regional ransomware trends: Over the past seven days, ZeroFox observed that North America was the region most targeted by ransomware attacks, followed by Europe and Russia and APAC. There were at least 62 ransomware attacks observed in North America, while Europe and Russia accounted for 34, APAC for 13, South America for 10, and Middle East and Africa for two.



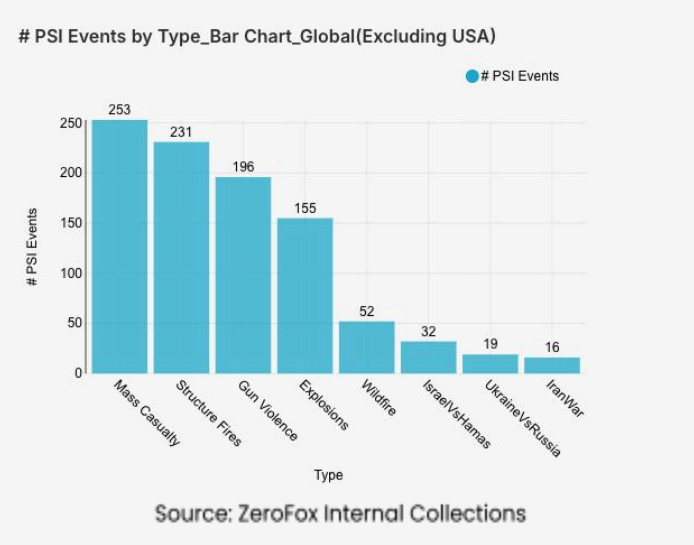
Source: ZeroFox Internal Collections

Notable Data Breaches of the Week

Targeted Entity	Aflac Japan	KDDI Corporation	Nissan
Compromised Entities/Victims	4.38 million Aflac Japan customers and insurance agents	14.22 million suspected current, former, and inactive customer accounts	Current and former Nissan employees in the United States, Canada, Mexico, and Brazil
Compromised Data Fields	Names, addresses, phone numbers, dates of birth, gender, security information, and insurance and premium transfer account information	Email addresses and passwords	Full names, Social Security numbers (SSNs), banking information, financial information, tax records/information, and possibly payroll and employee records
Suspected Threat Actor	N/A	N/A	ShinyHunters
Country/Region	Japan	Japan	Americas
Industry	Financial Services	Telecommunications	Automotive
Possible Repercussions	Identity theft, social engineering, insurance fraud, account takeover attempts, targeted phishing campaigns, and financial fraud	Credential stuffing, account takeover attacks, phishing, and Business Email Compromise (BEC)	Identity theft, financial fraud, phishing, and social engineering campaigns

Three major breaches observed in the past week

Physical and Geopolitical Intelligence Key Findings



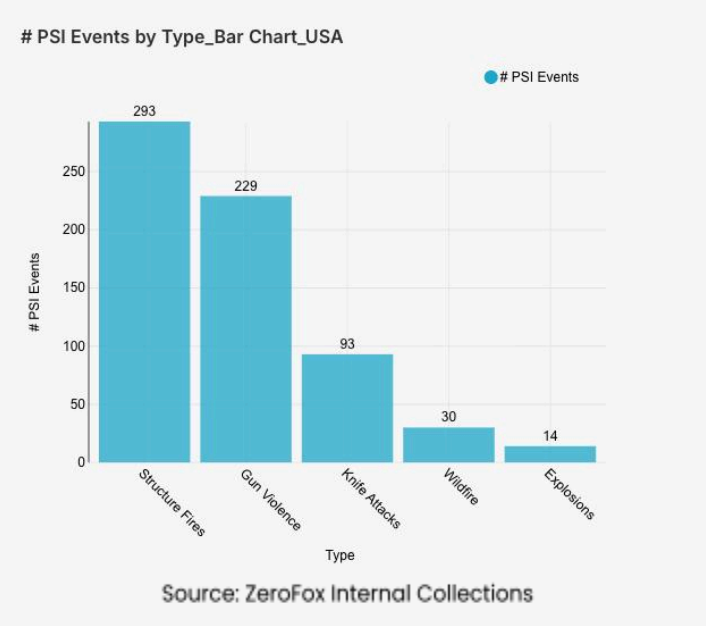
Source: ZeroFox Internal Collections

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 14 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being Mexico, Ukraine, and India, in that order. Approximately 61 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 24 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict did not increase or decrease from the previous week, and alerts related to the war in Iran decreased by 6 percent. Events related to Russia's war in Ukraine increased by 58 percent. The top three most-alerted subtypes were structure fires, which saw a 6 percent increase from the previous week; gun violence, which decreased by 7 percent; and explosions, which increased by 10 percent. Notably, wildfires increased by 73 percent from the previous week.

- **What this means:** Global mass casualty data this week is defined by conflict, organized crime, and escalating environmental disasters. In Ukraine, the spike in conflict-related alerts tracks with a significant intensification of Russia's air campaign, which included a drone and missile attack from July 1–2, killing at least 17 civilians and injuring many more in Kyiv. The day prior, Russian forces also launched several strikes on populated areas in Ukraine's Sumy region, injuring 21 people, while airstrikes on Zaporizhzhia killed two and injured 15. Ukraine also had the highest number of explosions this week, contributing to the increase in this subtype. The surge in wildfire alerts is exemplified by France; more than 1,000 hectares burned across simultaneous wildfires in southern France this week, with the largest blaze scorching over 800 hectares, prompting the evacuation of around 350 residents and the destruction of nearby vineyards. Taken together, this week's data is driven by the compounding pressures of armed conflict, criminal violence, terrorism, and increasingly severe climate-driven disasters.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were structure fires, gun violence, and knife attacks. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, knife attacks include confirmed stabbings or slashings, and structure fires are fires that affect man-made buildings. The top two states with the most gun violence alerts were Illinois and Ohio, which together made up 24 percent of this week's nationwide total. Gun violence across the United States overall decreased by 13 percent from the week prior. Knife attacks increased by 27 percent, and the top contributing states were California and Illinois. Structure fires decreased by 6 percent, and the top two states for this subtype were California and New York. Notably, explosions increased by 100 percent from the previous week.

- **What this means:** This past week's threat landscape across the United States underscored persistent patterns of violence and man-made disasters. While overall gun violence declined, deadly incidents continued to emerge across the country, with nine mass shootings occurring within the last week. For instance, one person was killed and six others were wounded in a mass shooting at an illegal street takeover in Carson, California, on June 28. Knife attacks surged nationally; in Hartford, Connecticut, two men were killed, and a 17-year-old was injured following a stabbing and shooting that erupted out of a large fight. Explosions doubled in frequency from the prior week, exemplified by an incident in Bucks County, Pennsylvania, where a historic farmhouse was deemed a total loss after a blast believed to be linked to a propane tank leak, with one contractor injured and taken to the hospital with burns. Rounding out the week's hazard picture, the National Interagency Fire Center elevated its National Preparedness Level to 4, with firefighters working to contain 51 uncontained large fires. Taken together, these incidents reflect the national convergence of urban violence, structural hazards, and unpredictable mass casualty events.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%